Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic

David Carlisle

Commentary, 2 March 2017

The enormous attention given to Bitcoin's rise has prompted security agencies to ponder whether cryptocurrencies could become a terrorist financing tool. A recent case suggests terrorists may be testing the waters. But overreaction could stifle an important new financial technology.

In January 2017, Indonesia's anti-money laundering/counter-terrorist finance (AML/CTF) agency provided the first specific, public allegations from a government of terrorists using cryptocurrencies.

According to Indonesian government sources, Bahrun Naim, a member of Daesh (also known as the Islamic State of Iraq and Syria, or ISIS), sent Bitcoin to fellow members across Indonesia to avoid transferring money through the formal financial system.

Is this a sign of a coming wave of terrorist financing using new technology? Is Bitcoin a menace that should be banned, as US Senator Joe Manchin advised in 2014?

The prospect of terrorists relying on cryptocurrencies – a subset of privately developed, tradable stores of digital value referred to as 'virtual currencies' – has prompted action from a number of jurisdictions.

The EU Parliament is expected to pass measures soon requiring the UK and other member states to bring certain virtual currency service providers within their AML/CTF regulation. These measures do not seek to prevent the use of cryptocurrencies, but will require virtual currency service providers to implement customer due diligence measures, just as banks do now.

Cryptocurrencies enable rapid and borderless transaction settlement on a 'peer-to-peer' basis. This means that network participants can transact directly without relying on a financial institution to process or settle the transaction.

In addition, cryptocurrencies contain various levels of pseudonymity or anonymity. In the Bitcoin network, users are identified not by their name, but by an alphanumeric public key.

Technologies that allow users to make rapid funds transfers outside the formal banking system and using concealed identities might seem to have enormous appeal to Daesh and other global terrorists.

In truth, however, the threat landscape presents a more muted picture; terrorist financing via cryptocurrencies is a risk that could grow with time, but one that warrants a measured response.

Available information on terrorists' use of cryptocurrencies is limited and anecdotal. In June 2015, the US charged a Daesh supporter for posting on Twitter about how others might use Bitcoin to fund the terror group. However, in that instance, there is no indication that actual transfers took place.

In August 2016, a former CIA analyst published findings identifying a Palestinian media organisation, the Ibn Taymiyyah Media Center, a Gaza-based online jihadist news agency – labelled by the US as having terrorist connections – as receiving small-value Bitcoin donations. Otherwise, and with the exception of Indonesia's announcement, the public record is unspecific and speculative.

Still, security agencies have focused on the possibility that cryptocurrencies' use in terrorism could grow. Terrorists are rapidly becoming more technologically adept. The head of Europol, Rob Wainwright, recently described terrorists as winning the online arms race, relying increasingly on social media and online platforms to generate support faster than law enforcement can keep pace.

As terrorists expand their online presence, security agencies worry their use of cryptocurrencies will expand. Governments are anxious about terrorists' use of the dark web – or encrypted portions of the web where users interact anonymously and where cryptocurrencies often feature.

Of particular concern to law enforcement agencies is the use of 'mixers' or 'tumblers'. These privacy-enhancing tools obscure the trail of cryptocurrency transactions and can stifle attempts to decipher financial activity.

Still, perspective is necessary. It is not yet clear whether cryptocurrencies will become a major terrorist funding tool, at least in the near-term, and the longer-term picture remains uncertain. Indeed, terrorists already have a number of reliable financing streams, which show little sign of drying up.

As Tom Keatinge and Florence Keen illustrate in a recent RUSI report, lone actor and small-cell terrorists fund their activity on a micro scale, using easily accessible financial services. This includes student and payday loans, public benefits, and cash.

These funding methods are often impossible for the financial sector or intelligence agencies to spot ahead of their use in terrorist operations. With such simple funding available, terrorists may not need to rush into cryptocurrencies.

Treating cryptocurrencies as an exceptional threat creates the misleading impression that more conventional financial products are not already equally, or more, vulnerable to terrorist exploitation.

What's more, banning Bitcoin or other cryptocurrencies could stifle important innovations that could enhance financial services. While it is still far from clear how significant an impact cryptocurrencies will have, a number governments, including the UK's, are keen to enable innovation in the sector.

Cryptocurrencies have particularly vocal champions among some proponents of financial inclusion, or expanding financial services to the world's poor. Cryptocurrencies' peer-to-peer nature enables transfers to occur at reduced cost compared to credit card transactions and other established payment methods that rely on numerous intermediaries.

Proponents argue cryptocurrencies could play a role in helping the unbanked to access cost-effective financial services.

Virtual currencies therefore offer governments a test case in harnessing the promise of technological innovation while also managing financial crime risks that are still only taking shape.

Countries should pursue a sensible approach. They should ensure their law enforcement agencies have the necessary resources and skills to uncover related illicit activity; and they can work to improve information sharing with their foreign counterparts on joint investigations.

Limited efforts at regulating certain cryptocurrency service providers, such as cryptocurrency exchanges, mark a reasonable initial attempt at oversight.

Countries should take time to monitor and assess the effectiveness of new regulation before rushing into further action.

As with any new technology, awareness of risks is critical. But overreaction and panic in this early stage in cryptocurrencies' history would be misguided.

David Carlisle is an independent consultant specialising in devising strategies for combating financial crime.

Banner image: If Bitcoins were real currency, this is perhaps what they would look like. Courtesy of Isokivi/Wikimedia.

Technical Decisions on Iran have made the Financial Action Task Force Political

Commentary, 5 March 2018

Tom Keatinge

The latest FATF plenary has drawn the financial technical standard-setter deep into uncomfortable political territory.

Tags: Iran's Nuclear Programme, AML/CTF, Iran

RUSI Research Project featured in UN Security Council Report

News, 2 March 2018

RUSI's Future of Financial Intelligence Sharing research programme was cited this week in a UN report on the threat posed by ISIL.The Secretary-General report addressed the ways in which the threat of ISIL. The sixth report of its kind, it considered how to prevent the financing of terrorism and how 'innovative partnerships between Government agencies and private sector actors' could help achieve...

Tags: Centre for Financial Crime and Security Studies, AML/CTF, Middle East and North Africa

Is a Corner Finally Being Turned in the UK's Fight Against a 'McMafia' World?

Commentary, 21 February 2018

Tom Keatinge and Florence Keen

A BBC TV drama might be the spur the UK government needs to take action on high-end money laundering.

Tags: AML/CTF, Organised Crime

1 2 3 4 5 6 7 8 9 ... NEXT › LAST »

RUSI
www.rusi.org

CORPORATE

Our corporate memberships will also offer you unique access into the defence and security community through networking opportunities and discounted conference fees.

Corporate

INDIVIDUAL

RUSI members enjoy privileged access to the RUSI Journal, Newsbrief and Defence Systems as well as invitations to our full programme of exclusive members' lectures and seminars. Members also have access to our renowned Library of Military History and online catalogue.

Individual

RUSI LIBRARY

The collection is dedicated to developing our knowledge of war and sharing theoretical approaches to modern military thinking... read more

Open 9:30AM - 4:30PM
Monday to Friday

Visit Library

SUBSCRIBE TO OUR NEWSLETTER

Receive updates on RUSI's research initiatives, publications and events, with highlights of commentary and analysis.

Subscribe

SUPPORT RUSI

Noted for its quality, RUSI's analysis is driven by an ethos of accuracy, objectivity and policy relevance.

Donate

LOCATIONS

London Whitehall
RUSI International
RUSI Japan
RUSI Qatar

INSIDE RUSI

Home
Login
Sign Up
FAQs
Contact Us
Legal
Privacy
Ethics